Chief Information Officer's Section
Office of the Governor
State of Utah

May 14, 2001

State Information Security Policy

1. Role of Information and Information Systems: Information and information systems are critical and vitally important State of Utah assets. Without reliable and properly secured information and information systems, the State of Utah business processes would be irreparably harmed. Likewise, the preservation and enhancement of State of Utah's reputation is directly linked to the way in which both information and information systems are managed. Maintaining an adequate level of security is one of several important aspects of both information management and information systems management.

To be effective, information security must be a team effort involving the participation and support of every State of Utah agency and employee who deals with information and/or information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of agencies and users as well as the steps they must take to help protect State of Utah information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

2. Scope: For the purposes of this policy, security is defined as the ability to protect the integrity, availability, and confidentiality of information held by agencies and to protect information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction. It includes the security of information technology facilities and off-site date storage; computing, telecommunications, and applications related services purchased from other state agencies or commercial concerns; and Internet-related applications and connectivity. Any entity physically connected to the WAN (Wide Area Network) of the State of Utah must comply with this policy or disconnect from the WAN.

2.1 Involved Persons: Provisions of this policy are applicable to all employees. Specific agency policies may be more restrictive. Every employee of the State of Utah, no matter what their status, merit or exempt, must comply with the information security policies found in this and related information security documents. Contractors and consultants are also required to comply with this security policy. Those who deliberately violate this and other information security policy statements will be subject to disciplinary action up to and including termination of employment or contracts.

2.2 Involved Systems: This policy applies to all computers, PDA's, network systems and data owned by and/or administered by State of Utah. Similarly, this policy applies to all platforms (operating systems), all computer sizes (personal computers through mainframes), and all application systems (whether developed in-house or purchased from third parties). The policy covers only information handled via computers and/or networks. Although this document includes mention of other media such as voice and paper, it does not directly address the security of information in these forms.

2.3 Involved Agencies: This policy applies to all executive branch agencies, as provided by law, that operate, manage or use information technology services or equipment to support critical state business functions.

3. Policy: It is the information security policy of the state of Utah that:

3.1 Each agency communicating over the State of Utah WAN shall operate in a manner consistent with the maintenance of a shared, trusted environment within state government for the protection of sensitive data and business transactions. Agencies may establish certain autonomous

applications, including those hosted by an Applications Service Provider or other third party, outside of the shared, trusted environment, provided the establishment and operation of such applications does not jeopardize the enterprise security environment, including:

- The security protocols (including means of authentication and authorization) relied upon by others; and,

- The integrity, reliability, and predictability of the State wide area network.

3.2 Each agency shall establish its secure state business applications within the existing Utah wide area network. This requires that all parties interact with agencies through a common security architecture and authentication process. The Division of Information Technology Services (ITS) shall maintain and operate the shared infrastructure necessary to support applications and data within a trusted environment.

3.3 Furthermore, each agency that operates its applications and networks within the Utah wide area network must subscribe to the following principles of shared security:

- Agencies must follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;

- Agencies must recognize and support the State's standard means of authenticating external parties needing access to sensitive information and applications;

- Agencies must follow security standards established for securing servers and data associated with the secure application; and

- Agencies must follow security standards established for creating secure sessions for application access.

3.4 Each agency must address the effect of using the Internet to conduct transactions for State business with other public entities, citizens, and businesses. Plans for Internet-based transactional applications, including but not limited to e-commerce, must be prepared and incorporated into the agency's information plans and submitted to the CIO and ITS for security validation.

3.5 Each agency must ensure staff is appropriately trained in information technology security procedures. Each agency must make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible. Agencies are encouraged to participate in appropriate security alert response organizations at the state and regional levels.

3.6 Each agency must review its information technology security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment. Examples of these changes include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.

3.7 Agency heads are responsible for the oversight of their respective agency's information technology security and will confirm in writing to the CIO that the agency is in compliance with this policy. An annual security verification letter may be included in the agency information technology plan submitted to the CIO. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as updates to them since the last approval.

4. Primary Agencies Working on Information Security: Pursuant to the State of Utah Information Security Charter, Guidance, direction, and authority for information security activities is vested in the CIO; and operational implementation of information security for all State of Utah executive agencies in the Division of Information Technology Services (ITS). This authority is

pursuant to the Governor's Executive Order dated December 11, 2001; *Utah Code 63A-6-103* and the Information Technology Act in *Utah Code 63D-1-105*. Provisions of the Government Records and Management Act (GRAMA) in *Utah Code 63-2 Part 2* also impact state security policies. The Information Technology Policy and Strategy Committee (ITPSC) through the actions of the State Information Security Committee (SISC) is vested with the responsibility for approving all statewide policies per the provisions of the Information Technology Act. ITS is responsible for maintaining enterprise-wide information security policies, standards, guidelines, and procedures as approved by the CIO. Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of the agency security managers and auditors and the State Auditor in terms of overall compliance issues. Investigations of system intrusions and other information security incidents are the responsibility of the agency security managers in conjunction with ITS. Local managers working in conjunction with the Department of Human Resource Management (DHRM) handle disciplinary matters resulting from violations of information security policies.

5. Security Standards and Requirements

5.1 Categories of Responsibilities: The State of Utah has identified three categories, at least one of which applies to each employee. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

5.2 Owner Responsibilities: Information Owners are the Agency Directors, Managers, and Executive Management, within State of Utah who bear responsibility for State of Utah information processed by production applications. Production applications are computer programs used by agencies to gather and analyze data pertinent to the business responsibilities of the agency. All production application system information must have a designated Owner. For each type of information, Owners designate the relevant sensitivity (e.g., public, protected or controlled), designate the appropriate level of criticality, define which users will be granted access, as well as approve requests for various ways in which the information will be utilized.

5.3 Custodian Responsibilities: Custodians are in physical or logical possession of either State of Utah information or information that has been entrusted to State of Utah. Custodians, such as information technology staff, will be clearly designated by Owners in writing. Wherever information is maintained, a custodial duty-of-care will be required of any individual entrusted with use of or access to State information resources. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

5.4 User Responsibilities: Users are those employees, contractors and external parties authorized to access and use data state owned data and programs. Users are responsible for familiarizing themselves with and complying with all State of Utah policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information. As information systems become increasingly integrated and distributed (through mobile computing, desktop computing, etc.), Users are increasingly placed in a position where they must handle information security matters that they did not handle previously. These systems force users to play security roles that they had not previously had to play.

5.5 Consistent Information Handling: State of Utah information, and information which has been entrusted to State of Utah, must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems, which process it (personal computers, firewalls, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Information must also be consistently protected no matter what its stage in the life cycle from origination to destruction.

5.6 Need-to-Know: Access to information in the possession of, or under the control of State of Utah must only be disclosed in a manner consistent with the policy established by the owner of the

information. In other words, information must be disclosed only when the Owner of the information in question instructs that it be shared. Information owners have certain responsibilities under the provisions of GRAMA concerning the disclosure of information and set policies and controls accordingly. Employees must not attempt to access sensitive information unless the relevant Owner has granted them access rights. When an employee changes job duties (including termination, transfer, promotion and leave of absence), his or her supervisor must immediately notify agency security, and LAN administrators. Employees with access to human resources information whose job duties have changed must also contact DHRM. The privileges granted to all employees will be periodically reviewed by information Owners and Custodians to ensure that only those with a current need-to-know presently have access.

5.7 Network User-IDs and Passwords: To implement the need-to-know process, the State of Utah insists that each employee accessing information systems have a unique network user-ID and a private password. These network user-IDs must then be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each employee is personally responsible for the usage of his or her network user-ID and password.

5.8 Anonymous Network User-IDs: With the exception of electronic bulletin boards, Internet web sites, Intranet Web sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any State of Utah system or network anonymously. Anonymous access might, for example, involve use of "guest" network user-IDs. When users employ system commands that allow them to change active network user-IDs to gain certain privileges, they must have initially logged-in employing network user-IDs that clearly indicated their identities. Exceptions may be allowed for system level and administrative ID's that are needed to provide specific system functionality.

5.9 Password Constraints: To make guessing more difficult, passwords must also be at least eight characters in length, including 1 numeric and 1 control character. Whenever an employee suspects that a password has become known to another person, that password must immediately be changed. Grace logins upon password expiration shall not exceed six.

5.10 Compliance Statement: All contractors or consultants wishing to use State of Utah computer systems must sign a compliance statement prior to being issued a network user-ID (See Appendix A.) or an equivalent document approved by the agency(s) where they are employed. All state of Utah employees should understand and agree to abide by State of Utah policies and procedures related to computers and networks (including the instructions contained in this policy).

5.11 Release of Information to Third Parties: Unless it has specifically been designated as public, all State of Utah internal information must be protected from disclosure to third parties. Third parties may be given access to State of Utah internal information only when a demonstrable need-to-know exists, and when such a disclosure has been expressly authorized by the relevant State of Utah information Owner. If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information Owner and ITS must both be notified immediately.

5.12 Third Party Requests for State of Utah Information: Requests for information are subject to the provisions of GRAMA. Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about State of Utah and its business must be referred to the information Owner. Custodians of information may not release information to any third party without the express permission of the information Owner.

5.13 Internal Network Connections: All State of Utah computers that store sensitive information, and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Division of Information Technology Services. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system. Computer users are advised to employ screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is

again entered. Similarly, information systems throughout State of Utah must employ automatic log-out systems that automatically terminate a user's session after a defined period of inactivity.

5.14 External Network Connections: All in-bound session connections to State of Utah computers from external networks (Internet, public dial-up lines, etc.) must be protected with an approved password access control system. Users with personal computers connected to external networks are prohibited from leaving unattended modems turned-on while data communications software is enabled. In general terms, State of Utah employees must not establish connections with external networks (including Internet Service Providers) unless the agency security managers and/or ITS have approved these connections. Such connections must not compromise security policies established with Internet firewalls or agency firewalls.

5.15 Network Changes: Changes to State of Utah internal networks include loading new communications software, adding new blocks of network addresses, changing the addresses of primary servers or domain controllers, reconfiguring routers, adding dial-up lines, and the like. With the exception of emergency situations, all changes to State of Utah computer networks that impact other agencies use of the State Wide Area Network or pose security risks must be: (a) documented in a work order request, and (b) approved in advance by the Division of Information Technology Services. The use of DHCP is not intended to be restricted by these provisions. Emergency changes to State of Utah networks must only be made by persons who are authorized by the Division of Information Technology Services. This process prevents unexpected changes inadvertently leading to denial of service, unauthorized disclosure of information, and other related problems. This process applies not only to "employees" as defined in the Scope section of this policy, but also to vendor personnel.

5.16 Security Sign-Off Required: Agency security managers, and/or ITS will approve the security controls of new or substantially changed application programs prior to releasing the systems into production.

5.17 External Disclosure of Security Information: Information about security measures for State of Utah computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the agency IT Director or Manager, or the Division of Information Technology Services has first been obtained. Public disclosure of electronic mail addresses is permissible.

5.18 Security Compromise Tools: Unless specifically authorized by agency IT Directors/Managers or agency security managers and the Division of Information Technology Services., State of Utah employees must not within the course and scope of employment functions acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security on State of Utah computer systems or networks. Examples of such tools include those, which defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Similarly, without this type of approval, employees are prohibited from using "sniffers" or any other hardware or software, which monitors the traffic on a network or the activity on a computer unless authorized to do so as a part of their employment responsibilities.

5.19 Prohibited Activities: Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by agency IT Directors/Managers or agency security managers and the Division of Information Technology Services. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, launching of denial of service attacks using State of Utah computing resources, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of State of Utah information security policy. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are prohibited.

5.20 Mandatory Reporting: All suspected policy violations, system intrusions, virus infestations, and other conditions, which might jeopardize State of Utah information or State of Utah information systems must be immediately reported to agency security managers, and when it

jeopardizes interagency systems or enterprise resources, be reported to the ITS security manager.

6. Security Guidelines and Recommendations

6.1 Difficult-to-Guess Passwords: To ensure that password systems do the job they were intended to do, users should choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang should not be used.

6.2 Easily Remembered Passwords: Users can choose easily remembered passwords that are at the same time difficult for unauthorized parties to guess if they:

(a) String several words together (the resulting passwords are also known as "pass phrases"),
(b) Shift a word up, down, left or right one row on the keyboard,
(c) Bump characters in a word a certain number of letters up or down the alphabet,
(d) Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word,
(e) Combine punctuation or numbers with a regular word,
(f) Create acronyms from words in a song, a poem, or another known sequence of words,
(g) Deliberately misspell a word (but not a common misspelling), or
(h) Combine several preferences like hours of sleep desired and favorite colors.

6.3 Repeated Password Patterns: Users should not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must NOT employ passwords like "JAN01" in January, "FEB02" in February, etc. Additionally, users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

6.4 Password Storage: Passwords should not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Similarly, passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons might discover them.

6.5 Sharing Passwords: If users need to share computer-resident data, they should use electronic mail, groupware databases, public directories on local area network servers, and other mechanisms. Although network user-IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. One exception to this involves expired passwords, which are received at the time a network user-ID is issued; these passwords must be changed the first time that the authorized user accesses the system. To share a password (or for that matter any other access mechanism such as a dynamic password token) exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. If an employee believes that someone else is using his or her network user-ID and password, the employee must immediately notify the security administrator for the information system in question.

6.6 Physical Security to Control Information Access: Access to offices, computer machine rooms, and other State of Utah work areas containing sensitive information must be physically restricted to those with a need-to-know. When not in use, sensitive information must always be protected from unauthorized disclosure.

6.8 Internet Access: Employees are generally provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of an employee's supervisor. The Office of the CIO reserves the right to filter Internet access to ensure that employees are not visiting web sites with inappropriate content, and to ensure that they continue to be in compliance with security policies and the State of Utah Acceptable Use Policy. Separately, employees should not place State of Utah material (software, internal memos,

databases, etc.) on any publicly accessible computer system such as the Internet unless the posting has first been approved by the information Owner.

6.9 Computer Virus Screening: Viruses can now spread by data files, not just by program files. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of personal computers and servers. To assure continued uninterrupted service for computers and networks, all personal computer users should keep the current versions of approved virus-screening software enabled on their computers. This screening software should be used to scan all software and data files coming from either third parties or other State of Utah groups. This scanning should take place before new data files are opened and before new software is executed. Employees should not bypass or turn-off the scanning processes which could arrest the transmission of computer viruses. The decision of what software will be used for virus screening is left to the discretion of the Information Owner in conjunction with agency security personnel and/or ITS.

6.10 Computer Virus Eradication: If employees suspect infection by a computer virus, they should immediately stop using the involved computer and call their agency LAN administrator or Help Desk. Floppy disks and other magnetic storage media used with the infected computer should not be used with any other computer until the virus has been successfully eradicated.

6.11 Clean Back-Ups: To assist with the post-virus-infection restoration of normal personal computer activities, all personal computer software should have the original media or a write protected backup copy stored in a secure location. These master copies should not be used for ordinary business activities, but should be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

6.12 Software Sources: To prevent problems with viruses, worms, and Trojan horses, State of Utah computers and networks should not run software that comes from sources other than: (a) other State of Utah departments, (b) knowledgeable and trusted user groups, (c) well-known systems security authorities, (d) established computer or network vendors, or (e) established commercial software vendors.

6.13 Written Specifications for Owners: All software intended to process critical or sensitive State of Utah information, should have a written specification. This specification must include discussion of both security risks and controls (including access control systems and contingency plans). The specification should be part of an agreement between the involved information Owner and the system developer. Macros in spreadsheets, word processing documents, and the like are not considered software for purposes of this paragraph.

6.14 Formal Change Control: All computer and communications systems used for production processing at the State of Utah should employ a documented change control process, which is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. This policy applies to personal computers running production systems, just as it applies to servers.

6.15 Back-Up Responsibility: To protect State of Utah's information resources from loss or damage, personal computer users are responsible for regularly backing-up the information on their personal computers, or else making sure that someone else is doing this for them. For server based computer and communication systems, the Information Owner/Custodian is responsible for making periodic back-ups. If requested by the agency IT director/manager, the Division of Information Technology Services will install, or provide technical assistance for the installation of back-up hardware and/or software. All back-ups containing critical and/or sensitive information should be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information; it is the responsibility of the information Owner to make sure that this plan is adequately developed, regularly updated, and periodically tested.

6.16 Theft Protection: All State of Utah computer and network equipment should be physically secured. Servers and related equipment should be placed in locked cabinets, locked closets, or locked computer rooms. Computer and network equipment may not be removed from State of Utah offices unless the involved person has first obtained a property pass from the building manager. Pagers, laptops, PDA's and cellular phones are not subject to these requirements.

6.17 Right to Search and Monitor: To ensure compliance with State of Utah internal policies as well as applicable laws and regulations, and to ensure employee safety, State of Utah management reserves the rights to monitor, inspect, and/or search at any time all State of Utah information systems. This examination may take place with or without the consent, presence, or knowledge of the involved employees. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voicemail files, printer spool files, and other data storage devices. All searches of this nature will be conducted after the approval of appropriate agency management, and/or legal counsel. Since the State of Utah's computers and networks are provided for business purposes only, employees should have no expectation of privacy associated with the information they store in or send through these information systems. State of Utah management additionally retains the right to remove from its information systems any material it views as offensive or potentially illegal subject to the current Acceptable Use Policy.

References:

Interim Date: January 8, 2001
Organization Sponsoring the Standard: State Information Security Committee (SISC)
State Technical Architect Approval Date: Pending
CIO Approval Date: Pending
ITPSC Presentation Date: January 18, 2001, December 20, 2001
Author(s): Robert Woolley (ITS)
Related Documents: Governor's Executive Order of December 11, 2001**,** State Information Security Charter, State Acceptable Use Policy, Utah Administrative Rule R365-4 "Information Technology Protection," Rule R365-3 "Computer Software Licensing, Copyright, and Control," Policy for Limiting Access to Inappropriate Web Sites, Privacy Policy – State Web Sites, and the State Telecommuting Policy.

Appendix A.
Agreement To Comply With Information Security Policies

A signed paper copy of this form must be submitted with all requests for (1) authorization of a new network user-ID, (2) authorization of a change in privileges associated with an existing network user-ID, or (3) any periodic reauthorization of an existing network user-ID. Modifications to the terms and conditions of this agreement will not be accepted.

User Printed Name: _____

User Agency Name: _____

User Telephone Number: _____

User's Office Physical Address: _____

_____

_____

_____

I, the user, agree to take all reasonable precautions to assure that State of Utah internal information, or information which has been entrusted to the State of Utah by third parties (such as clients, or vendors), will not be disclosed to unauthorized persons. At the end of my employment or contract with the State of Utah, I agree to return to The State of Utah all information to which I have had access in order to do my job. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal State of Utah manager who is the designated information owner.

I have access to a copy of the State of Utah Information Security Policies, I have read and understand these materials, and I understand how they impact my job. As a condition of continued employment at The State of Utah, I agree to abide by these information security policies. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, or termination of employment.

I agree to choose a difficult-to-guess password as described in the State of Utah Information Security Policies document, I agree not to share this password with others, and I agree not to write the password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the agency IT manager or security manager or the ITS security manager.

User Signature: _____ Date: _____